Attachment 2a

FCC Computer System Application Access Assignment Form

Employees and contractors who are requesting application access must have this form completed and returned to the Application Owner. Access must be granted in accordance with FCC Instruction 1479.2 Computer Security Program Directive.

USER INFORMATION

(To be completed by Application Owner)

User Name (*Print Last, First MI*):	User Name ID:
Bureau/Office or Contract Name:	Date Access Required:
Major Application Access:	Access Level:

APPLICATION RULES OF BEHAVIOR ACKNOWLEDGEMENT

(To be completed by user and returned to Application Owner when Completed)

I have received a copy of the attached Application Rules of Behavior that provide information on Federal regulations, user responsibilities and the consequences of my actions, and computer security policies and procedures. I have read and will fully comply with the rules in their entirety. I recognize that it is my responsibility to ensure that I comply with the Federal computer security policies and procedures described in the FCC Computer Security Program Directive.

Printed Name: ______________________ Organization: ______________________

Signature: ______________________ Date: ______________

ACCESS APPROVAL

I am aware that the following access has been granted to this userID:

□ Privileged, Administrative Account. □ Non-Privileged, Non-Administrative User Account

Supervisor or COTR (*Printed Name*): **Ruth A Dancey, COTR**	Signature:	Date:
Application Security Custodian (*Printed Name*):	Signature:	Date:

Return this form to the Computer Security Officer, Room 1-A325
445 12th Street, S.W., Washington, DC 20554

APPLICATION RULES OF BEHAVIOR

Passwords:

- □ Passwords must be at least characters long.
- □ Do not write down passwords.
- □ Do not share your passwords or accounts with others.
- □ Enable a password protective inactivity screensaver at your station.
- □ Passwords are to be changed every days.
- □ Use paraphrases instead of dictionary words when creating passwords.

Electronic Data/Media and Paper:

- □ Do not post system sensitive material in areas subject to public traffic or viewing (offices next to windows on ground floors please take special note).
- □ Do not transport system sensitive material in an unprotected manner.
- □ Lock down all sensitive unclassified material when leaving your work area.
- □ Protect sensitive unclassified information from alteration, disclosure or loss.
- □ Ensure all storage media are reformatted before they are removed for storage in a protected environment.
- □ Ensure that appropriate warning labels are printed on each and every page of the sensitive documentation.
- □ Prevent dumpster diving--do not discard system sensitive materials or communications in public trash containers.
- □ Deleting a file does not remove its data from the media. Use utilities which delete with overwriting before releasing media for other assignments or to ensure its destruction.
- □ Access only information for which you are authorized, "need to know/access."
- □ Respect the copyright on the material you reproduce.
- □ Backup data files at frequent intervals.
- □ Respect and protect the privacy and confidentiality of records and privacy act information while in your custody.

Dial in Access:

- □ Dial in users must ensure that adequate safeguards are in place on the remote computer to ensure the security of the system to which you are dialing in to.
- □ Lock your terminal or log off if you must leave the work area even briefly.

Laptops:

- □ Login IDs, passwords and /or sensitive information should not be saved on the hard drive. Use a diskette/CD to save information.
- □ Protect passwords and user ID's from hacker, electronic eavesdroppers or shoulder surfers.

Internet Usage:

- □ Do not transmit sensitive information via the internet.
- □ Keep your anti-virus software current.
- □ Periodically virus scan your client.
- □ Virus scan all e-mail attachments.
- □ Do not open executable attachments.

General:

- □ Use FCC computing resources when accessing applications in a manner consistent with its intended purpose.
- □ Report sensitive circumstances to the help desk.
- □ Politely challenge unescorted visitors in your area (request identification and purpose).
- □ Be alert to the risk of theft, espionage and intrusion in the areas you work in and take appropriate countermeasures.
- □ Attend or participate in annual information security training.
- □ Report violations of security policies or procedures that come to your attention.
- □ Prevent social engineering–do not reset passwords for any person via telephone until the identity of the requestor has been confirmed and verified.
- □ Do not divulge account access procedure to any unauthorized user.
- □ Users are not permitted to override technical and management controls.

FCC Computer System
User Rules of Behavior

POLICY FOR USE OF COMPUTER RESOURCES.

As an employee or contractor of the Federal Communications Commission (FCC), you are required to be aware of, and comply with the FCC's policy on usage and security of computer resources, per OMB Circular A-130, Appendix III. Use of this system is for FCC authorized purposes only. Any other use may be misuse of Government property in violation of Federal regulations. All information in this system is subject to access by authorized FCC personnel at any time. Individual users have no privacy interest in such information.

YOU ARE RESPONSIBLE FOR ALL ACTIONS PERFORMED WITH YOUR PERSONAL USER ID.

- UserIDs and passwords are for your individual use only, and are confidential FCC information.
- You must not disclose your password to anyone. Furthermore, you must take necessary steps to prevent anyone from gaining knowledge of your password.
- Your UserID and password must be used solely for the performance of your official FCC job functions. (Refer to 5 CFR Part 2635, "Standards of Ethical Conduct for Employees of the Executive Branch.")

POLICY, STANDARDS, AND PROCEDURES MUST BE FOLLOWED.

- Use of all computer resources, including personal computers, laptops, all parts of the FCC Network, communication lines, and computing facilities are restricted to FCC-authorized purposes only.
- You must be aware of, and abide by the "Computer Fraud and Abuse Act of 1986" (Public Law 99-474), the civil and criminal penalties of the Privacy Act, the Trade Secrets Act (18 U.S.C. S905), and other Federal Regulations applying to unauthorized use of FCC files, records, and data. Training will be provided to educate you about your responsibilities under these statutes.
- Be aware that all computer resources assigned, controlled, accessed, and maintained by FCC employee and contractor personnel are subject to periodic test, review, and audit.

ACCESS TO INFORMATION MUST BE CONTROLLED.

- Access only the information for which you are authorized, and have "need to know/access."
- Do not leave computers logged on and unattended. Log off, use "lock workstation" feature, or use access control software (i.e., Screen Saver with password) during unattended use.
- If you know that a person, other than yourself, has used or is using your userID, you must report the incident immediately to your supervisor and the Computer Security Officer.
- Take steps necessary to maintain security of computer files and reports containing FCC information.

YOU ARE RESPONSIBLE FOR THE PROPER USE OF YOUR COMPUTER RESOURCES.

- Only use FCC-approved software, and comply with vendor software license agreements.
- Back up your programs and data on a regular basis, and do not store sensitive or mission-critical data on your PC's hard drive.
- All FCC computer resources, including hardware, software, programs, files, paper reports, and data are the sole property of the FCC.

USER CERTIFICATION

I certify that I have read the above statements, fully understand my responsibilities, and agree to comply.
I recognize that any violation of the requirements indicated above may be cause for disciplinary actions.

Name (please print): ______________________________

Signature: ______________________________ Date: ______________

Return this form to: Computer Security Officer, Room 1-A325

FCC Computer System
Separation Clearance

Employees and contractors who are separating from the FCC must have this form completed and delivered to the Network Development Group prior to their last day of work.

USER INFORMATION

User Name (Print First, MI, Last):	UserID:
Bureau/Office or Contract Name:	Separation Date:

CLEARANCE CERTIFICATION

I have been authorized access to FCC Computer Resources. By signing this form, I am severing all access rights to FCC computer systems and information therein, and have returned all information and electronic resources (e.g., portable computer(s), computer software and electronic reference materials, computer hardware, etc.).

User Signature: ______________________________ Date: ______________________

SUPERVISOR/COTR/ABC/DALO CLEARANCE

FCC Supervisor or COTR

I am aware that all files owned by this userID need to be transferred upon separation of user.

□ Retain and forward files to new userID: ____________________ or

□ Transfer files to diskette and call: ____________________ at (   ) __________ for pick-up, or

□ Purge files without transfer or copying to diskette.

Print Name: Signature/Date:

ABC Print Name:	Signature/Date:
Bureau/Office DALO Print Name:	Signature/Date:

Return this form to: Computer Security Officer, Room 1-A325
445 12th Street, SW, Washington, DC 20554